چگونه با بدافزار Backdoor.MAC.Eleanor در مک مقابله کنیم؟ - دیجیاتو

امین بیگ‌زاده | یکشنبه، ۲۷ تیر ۱۳۹۵

هفته گذشته کمپانی Bitdefender اعلام کرد که محققانش بدافزار جدیدی کشف کرده اند که می تواند امنیت رایانه های مک را به مخاطره بیندازد. گفته شده این بدافزار که Backdoor.Mac.Eleanor نام دارد، می تواند کنترل کامل سیستم شما را در دست گرفته تا با استفاده از آن هکرها بتوانند به دزدی اطلاعات و کنترل وب کم شما پرداخته و حتی از اجرای دستورات شما به رایانه جلوگیری کنند.

اما شیوه نفوذ و نحوه عمل این بد افزار چگونه است؟ از کجا باید فهمید که یک رایانه مک به آن آلوده شده؟ برای رسیدن به پاسخ تا پایان مقاله همراه ما باشید.

چگونه به سیستم نفوذ می کند؟

هکرها همیشه برای نفوذ، به دنبال روزنه هایی می گردند که در آن با کمترین مقاومت ممکن مواجه شوند، و در بسیاری از موارد این روزنه ها کاربران ناشناس هستند.

نحوه نفوذ Backdoor.MAC.Eleanor تفاوت چندانی با بدافزارهای دیگر ندارد. این بدافزار خود را پشت یک اپلیکیشن تبدیل فایل به ظاهر معتبر، اما تقلبی به نام **EasyDoc Converter** پنهان کرده و به بهانه نصب آن به سیستم شما نفوذ می کند.

صدور اجازه نصب برای EasyDoc کافیست تا بدافزار وارد سیستم عامل شده و شروع به اجرای کُد مخربی کند که موجب نصب یک سرویس مخفی Tor در سیستم می شود. حالا به واسطه این سرویس، هکرها می توانند از راه دور کنترل کامل رایانه مک شما را در دست بگیرند.

راه اندازی این سرویس مخفی تحت وب سبب می شود تا هکرها بتوانند از طریق آن فایل هایتان را بدزدند، جلوی دستورات شما به سیستم عامل را گرفته و به فهرستی از اپلیکیشن ها و فرآیندهای در حال اجرا دسترسی داشته باشند.

نکته بدتر اینکه می توانند حتی بدون اجازه شما به ارسال ایمیل به همراه فایل پیوست نیز اقدام بکنند. این بدافزار حتی می تواند با استفاده از ابزاری موسوم به wacaw کنترل وب کم رایانه مک شما را در دست گرفته و برای هکر امکان عکاسی و فیلمبرداری با آن را نیز فراهم نماید.

بیت دفندر هشدار داده که هکرها با این بدافزار می توانند کنترل لپ تاپ را به طور کامل از دست

شما درآورند، از شما اخاذی کرده یا لپ تاپ تان را به یک Botnet برای حمله به دستگاه های دیگر تبدیل کنند.

وجودش را چگونه تشخیص دهیم؟

خوشبختانه این بدافزار برای ورود به سیستم راه نفوذی به غیر از دانلود و نصب اپلیکیشن تقلبی EasyDoc Converter ندارد. رایانه های مک یک گزینه امنیتی به نام **Gatekeeper** در قسمت System Preferences و در تنظیمات Security & Privacy خود دارند. در حالت پیش فرض، این گزینه از اجرای اپلیکیشن های تأیید نشده توسط اپل جلوگیری به عمل می آورد.

در صورت فعال بودن این گزینه، اگر اپلیکیشنی را از منبعی به جز اپ استور مک دانلود و آن را نصب کنید، با هشداری مبنی بر غیر قابل اجرا بودن آن مواجه خواهید شد. هر چند که می توانید این هشدار را نادیده بگیرید.

اگر تا به حال اپ EasyDoc Converter را دانلود نکرده و Gatekeeper را برای اجرایش دور نزده باشید، امکان ندارد که رایانه مک شما به بدافزار Backdoor.MAC.Eleanor آلوده شده باشد. اما در غیر این صورت رایانه تان را صد در صد آلوده به این بدافزار بدانید.

چگونه آن را از سیستم عامل حذف کنیم؟

اگر از آلودگی رایانه تان به این بدافزار مطمئن شده اید، اما هنوز دسترسی تان به آن کاملا قطع نشده، خوشحال باشید. بسیاری از نرم افزارهای آنتی ویروس مک طی روزهای گذشته برای تشخیص و حذف Backdoor.MAC.Eleanor بروزرسانی شده اند. از جمله بهترین آن ها نرم افزارهای **Malwarebytes** و **Sophos Home** هستند که می توانند به سرعت سیستم را اسکن کرده و کلک این بدافزار مخرب را از آن بکنند.

برای پیشگیری از وقوع مجدد مشکلاتی این چنینی، بهتر است که در تنظیمات امنیتی مک گزینه Gatekeeper را فعال کنید تا فقط به اپلیکیشن های تأیید شده توسط اپل که در اپ استور مک موجودند اجازه نصب بدهد. اگر هم می خواهید اپلیکیشن توسعه دهنده ناشناسی را نصب کنید، حتما پیش از این کار از قابل اعتماد بودن منبع آن اطمینان حاصل کنید.

ضمنا بد نیست که در کنار نرم افزارهای آنتی ویروس، از اپلیکیشنی مثل BlockBlock هم برای تشخیص موارد مشکوک استفاده کنید. BlockBlock نه تنها می تواند بدافزارهای موجود در سیستم را برایتان شناسایی کند، بلکه اپلیکیشن های دارای محتوای مشکوک را هم به خوبی تشخیص می دهد. حتما از این نرم افزار در کنار Malwarebytes استفاده کنید و ترجیحا از دانلود اپلیکیشن ها از منابع نامعتبر بپرهیزید.

در میان تمام روش های حذف Backdoor.MAC.Eleanor، بهترین راه این است که یا OS X را مجددا نصب کرده و یا سیستم را به یکی از نسخه های پشتیبان Time Machine بازگردانی (ری استور) کنید. مراحل انجام این کار به شرح زیر هستند:

- مک را برای دسترسی به بخش Recovery خاموش کنید.
- موقع روشن کردن مجدد دستگاه، حالا دکمه های Command و R را با هم نگه داشته و به محض پدیدار شدن لوگوی اپل آن ها را رها کنید.
- اگر در Time Machine نسخه پشتیبان داشتید، گزینه ای را انتخاب کنید که تاریخ آن به پیش از نصب اپلیکیشن EasyDoc Converter باز می گردد.
- اگر هیچ نسخه پشتیبانی در Time Machine ندارید، بهتر است که گزینه Reinstall OS X را بزنید و سیستم عامل را مجددا نصب نمایید. توجه داشته باشید که با این کار کلیه اطلاعات ذخیره شده در هارد دستگاه از جمله تصاویر، اسناد و ... را از دست خواهید داد.
- منتظر ری استور شدن یا اتمام نصب سیستم عامل در دستگاه بمانید. پس از راه اندازی مجدد سیستم، بهتر است نخستین کاری که می کنید نصب یک نرم افزار آنتی ویروس مطمئن باشد.

دیجیاتو